New California Privacy and Security Laws Impose Nationwide Compliance Obligations (and Litigation Risks)

*by Ian C. Ballon**

Introduction

California has enacted four laws governing the collection of information from California residents that businesses that operate on a nationwide basis must comply with. First, California's Online Privacy Protection Act of 2003,[1] which took effect on July 1, 2004, requires operators of commercial websites and online services that collect personally identifiable information about California residents over the Internet or online to conspicuously post a privacy policy that includes specific information mandated by the statute. Second, California Civil Code sections 1798.83 and 1798.84, which took effect on January 1, 2005, require businesses that disclose personal information to third parties for direct marketing purposes to make certain disclosures to consumers and, upon request, provide them with details about the specific information disclosed about them. Third, California Civil Code section 1798.81.5, which took effect on January 1, 2005, requires most businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification or disclosure, and to contractually bind third parties who obtain this information to maintain reasonable security procedures. Fourth, California's security reporting statute,[2] which took effect on July 1, 2003, compels businesses under certain circumstances to notify consumers in the event of hacker attacks or other security breaches.

The new laws governing the privacy and security of personal information collected from consumers compels businesses that attract California residents to their sites to (1) post or potentially revise their privacy policies, (2)amend contracts with any third parties that obtain access to such information, (3) change their internal practices and procedures to ensure that they afford consumers the opportunity to learn about how their information is used and (4) notify consumers in the event of security breaches.

The laws impose new compliance obligations on businesses that collect information on their websites and potentially puts them at risk of litigation in California in the event they fail to properly implement the new laws (or in the case of the security notification statute—simply by virtue of complying with it).

The Obligation to Conspicuously Post a Privacy Policy (California's Online Privacy Protection Act of 2003)

Operators[3] of commercial websites and online services that collect personally identifiable information[4] over the Internet about individual consumers[5] residing in California who use or visit the site or service must conspicuously post[6] a privacy policy on their websites[7] (or in the case of service providers, by any other reasonably accessible means of making the policy available for consumers of their service[8]). The policy must:

- Identify the categories of personally identifiable information that the operator collects through the website or online service about individual consumers who use or visit its site or service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information;
- Describe the process by which an individual consumer may review and request changes to any personally identifiable information collected, if the operator provides such an option to consumers;[9]
- Describe the process by which the operator will notify consumers who use or visit its site or service of material changes to the policy; and
- Identify its effective date.[10]

Liability under the statute may be imposed if the operator "knowingly and willfully" or "negligently and materially" fails to comply with these statutory requirements *or with the terms of its posted policy.*[11] An operator will be deemed

***** *Named one of the top 25 intellectual property lawyers in California in 2003 by The Daily Journal, Mr. Ballon is the firm-wide co-chair of Manatt's Intellectual Property and Internet Practice Group. He represents technology, media, and entertainment companies in complex litigation and counseling and is the author of E-Commerce and Internet Law: A Legal Treatise with Forms (Glasser LegalWorks 2001 & Current Supp.). He also serves as Executive Director of Stanford University's Center for E-Commerce. He can be contacted at <iballon@manatt.com>. This article was excerpted from the 2004-2005 annual update to E-Commerce and Internet Law: A Legal Treatise with Forms, published by Glasser LegalWorks, <www.ballononecommerce.com>.*

to be in violation of this law if it fails to post a policy in compliance with the law within 30 days of being notified of noncompliance.[12]

Businesses that do not collect personally identifiable information online, or which do not collect such information from California residents, need not comply. As a practical matter, however, all other businesses that collect personally identifiable information online should comply with the statute since there is likely no way that a business could reliably exclude California residents.

Although most large consumer-oriented websites already posted privacy policies, there generally was no obligation to do so (outside of the financial services and health care industries or sites or services directed at children) prior to the adoption of this law.

Most established businesses that already have privacy policies posted on their sites likely were already in compliance with most of the provisions of the law. Many sites, however, did not otherwise identify an "effective date." Some businesses that could not determine the actual date their current policies took effect opted to list an effective date of "July 1, 2004," which was the day the statute took effect.[13]

The Obligation to Disclose Personal Information Transfers to Third Parties

California Civil Code section 1798.83 provides that if a business with 20 or more full or part-time employees[14] has an established business relationship[15] with a customer[16] and has within the immediately preceding calendar year disclosed[17] specified categories[18] of personal information (or certain information derived from this information[19]) to third parties,[20] and if the business knows or reasonably should know that the third parties used the personal information for their own direct marketing purposes,[21] the business shall, upon request[22] once per calendar year,[23] provide the customer free of charge (in writing or by email) within thirty (30)[24] days:

- a list of the categories disclosed for third party direct marketing purposes during the immediately preceding calendar year, and
- the names and addresses of all of the third parties that received such information and, if the nature of the third parties' business cannot reasonably be determined from their names, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business[25]

The obligations under this statute may be avoided if a business otherwise required to comply with the statute (1) adopts and discloses to the public in its privacy statement a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing such information if the customer has "exercised an option that prevents that information from being disclosed to third parties for those purposes," (2) maintains and discloses this policy, (3) notifies the customer of his or her right to prevent disclosure of personal information, and (4) provides the customer with a cost free means to exercise this right.[26]

However well intended, the effect of the disclosure law could be harsh for California businesses.

The law also includes a non-exclusive list of disclosures (in subdivision (d)) that are not deemed to be disclosures of personal information by a business for a third parties' direct marketing purposes for purposes of the statute:

- Disclosures between a business and a third party pursuant to contracts or arrangements pertaining to any of the following:
    - The processing, storage, management, or organization of personal information, or the performance of services on behalf of the business during which personal information is disclosed, if the third party that processes, stores, manages, or organizes the personal information does not use the information for a third party's direct marketing purposes and does not disclose the information to additional third parties for their direct marketing purposes.
    - Marketing products or services to customers with whom the business has an established business relationship where, as a part of the marketing, the business does not disclose personal information to third parties for the third parties' direct marketing purposes.
    - Maintaining or servicing accounts, including credit accounts and disclosures pertaining to the denial of applications for credit or the status of applications for credit and processing bills or insurance claims for payment.
    - Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in Section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in Section 1087, and not provided directly by the customer to a business in the course of an established business relationship.
    - Jointly offering a product or service pursuant to a written agreement with the third party that receives the personal information, provided that all of the following requirements are met:
        - The product or service offered is a product or service of, and is provided by, at least one of the businesses that is a party to the written agreement.
        - The product or service is jointly offered, endorsed, or sponsored by, and clearly and conspicuously identifies for the customer, the businesses that disclose and receive the disclosed personal information.

- The written agreement provides that the third party that receives the personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a product or service that is the subject of the written agreement.

- Disclosures to or from a consumer reporting agency of a customer's payment history or other information pertaining to transactions or experiences between the business and a customer if that information is to be reported in, or used to generate, a consumer report as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act.
- Disclosure of personal information by a business to a third party financial institution solely for the purpose of the business obtaining payment for a transaction in which the customer paid the business for goods or services with a check, credit card, charge card, or debit card, if the customer seeks the information required by subdivision (a) of the business obtaining payment, whether or not the business obtaining payment knows or reasonably should know that the third party financial institution has used the personal information for its direct marketing purposes.
- Disclosures of personal information between a licensed agent and it is principal, if the personal information disclosed is necessary to complete, effectuate, administer, or enforce transactions between the principal and the agent, whether or not the licensed agent or principal also uses the personal information is used by each of them solely to market products and services directly to customers with whom both have established business relationships as a result of the principal and agent relationship.
- Disclosures of personal information between a financial institution and a business that has a private label credit card, affinity card, retail installment contract, or co-branded card program with the financial institution, if the personal information disclosed is necessary for the financial institution to maintain or service accounts on behalf of the business with which it has a private label credit card, affinity card, retail installment contract, or branded card program, or to complete, effectuate, administer, or enforce customer transactions or transactions between the institution and the business, whether or not the institution or the business also uses the personal information for direct marketing purposes, if that personal information is used solely to market products and services directly to customers with whom both the business and the financial institution have established business relationships as a result of the private label credit card, affinity card, retail installment contract, or co-branded card program.[27]

In addition to the exemptions created by subdivision (d), the statute, by its terms, does not apply to a financial institution that is subject to the California Financial Information Privacy Act,[28] subject to certain limitations.[29]

The statute also contains special, less demanding rules for disclosures of personal information for direct marketing purposes between affiliated third parties that share the same brand name.[30]

California's new privacy and security statutes effectively impose national standards on businesses. . . .

Customers injured by violations of section 1798.82 may initiate a civil action to obtain injunctive relief and/or damages of up to $500 per violation (or $3,000 per violation for violations that were willful, intentional or reckless).[31] Unless a violation is willful, intentional or reckless, a complete defense is provided if, within 90 days of the business learning that it had failed to provide requested information, failed to provide complete or accurate information, or failed to provide the information in a timely fashion, the business fully provides complete and accurate information.[32] In addition to damages, the statute provides that injunctive relief may be obtained against any business that violates, proposes to violate or has violated the statute.[33]

In the event of litigation, a prevailing plaintiff (but not a prevailing defendant) shall be entitled to recover reasonable attorneys' fees and costs.[34]

The requirements of this statute are may not be waived. Any purported effort to waive rights created by section 1798.83 will be treated as void and unenforceable.[35]

California's Security Notification Statute

California's security reporting statute,[36] which took effect on July 1, 2003, establishes a notification procedure to deter security breaches and encourage careful pre-planning by companies, as well as to protect consumers in the event of breach.

The statute requires a state agency or a person or entity that conducts business in California and owns or licenses computerized data that includes personal information, to disclose in specified ways any security breach[37] to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The statute, which preempts any local regulations, also requires an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any security breach.

Under the statute, personal information means an individual's first name, or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) social security number; (2) driver's license number or California identification card number; (3) account, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Notice, under the statue, may be provided by: (1) written notice; (2) electronic notice, if consistent with the provisions governing electronic records and signatures set forth in the federal eSIGN law;[38] or (3) substitute notice, if the person, business, or agency demonstrates that the cost of providing actual notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the person, business, or agency does not have sufficient contact information to provide actual notice. Substitute notice must include: (A) email notice, if the person, business, or agency has an email address for a person; (B) a conspicuous website posting; or (C) notification through "major" statewide media. Notification may be delayed, however, if a law enforcement agency determines that it would impede a criminal investigation.

Low potential recoveries also may serve as a deterrent to litigation.

While the threat of compelled notification undoubtedly encourages businesses that might not otherwise do so to provide adequate security for customer information, even the best system may be breached by a hacker or as a result of human error. However well intended, the effect of the disclosure law could be harsh for California businesses. Notifications under California's security reporting statute could lead to litigation under California's notoriously broad Unfair Competition Statute (provided actual damages are alleged),[39] including potentially class action litigation. Regardless of when or how they arrive, notifications, in addition to alerting consumers, may generate adverse publicity and attract the attention of plaintiff's lawyers.

The Obligation to Implement and Maintain Reasonable Security Procedures

Eighteen months after California's security notification statute took effect, California Civil Code section 1798.81.5 became effective. That statute provides that a business that owns or licenses[40] personal information[41] about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.[42]

The statute also mandates that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

Like the security notification statute, section 1798.81.5 neither compels specific practices nor affords safe harbor protections. An alleged violation likewise could form the basis for a section 17200 class action suit. While the statute is flexible enough to protect consumers as "reasonable" security procedures and practices change over time, the lack of definition could serve as an invitation to litigation any time a security procedures and practices in fact are breached.

Conclusion

California's new privacy and security statutes effectively impose national standards on businesses—wherever they may be based—that collect personal information from California residents. By posting a privacy policy in compliance with California law, a site owner or service provider effectively subjects itself to FTC enforcement actions to the extent that it fails to comply with the representations made in its policy. More alarming for businesses, however, is the possibility that the new California laws could lead to litigation, including consumer class action suits.

To limit the risk of liability, businesses should conduct a privacy and security audit.

Disclosures of personal information at variance with a company's privacy policy—including disclosures that result from unintended security breaches—may lead to litigation under state tort, unfair competition or consumer protection laws. Privacy-related class action suits to date, while expensive to defend, generally have not yielded large settlements or judgments. Federal privacy statutes contain minimum damage requirements and other technical requirements that may be difficult to meet in litigation arising out of online consumer transactions, and generally are targeted at deterring hacking or other computer crimes rather than consumer protection.[43] Low potential recoveries also may serve as a deterrent to litigation. In addition, certification of a privacy or security-related class action may be difficult to obtain where users enter into a binding click-through or other agreements that provide for binding arbitration of disputes[44]—but only to the extent such agreements are deemed to be enforceable,[45] binding contracts.[46]

While privacy violations generally have not yielded significant damage awards or settlements, security violations could prove to be a more fertile area of growth for plaintiffs' class action lawyers because of the potentially greater damages that may accrue in certain kinds of security breach cases. California's security notification statute—in addition to warning consumers—serves to alert class action lawyers to potential claims.

To limit the risk of liability, businesses should conduct a privacy and security audit. Many companies will have to revise their internal practices and procedures—as well as their external policies and third party contracts—to ensure compliance with California's new laws and limit the risk of class action litigation. To be effective, privacy policies must reflect actual practices. Ultimately, however, businesses must properly educate key decision makers about the importance of privacy and security and ensure close coordination among their marketing, I.T. and legal departments. ●

1 Cal. Bus. & Prof. Code §§ 22575 *et seq.*

2 Cal. Civ. Code §§ 1798.29, 1798.82.

3 The term *operator* means

> any person or entity that owns a website located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the website or online service if the website or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a website or online service in the owner's behalf or by processing information on behalf of the owner.

Cal. Bus. & Prof. Code § 22577(c).

4 The term *personally identifiable information* means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including the following:

> (1) A first and last name.
> (2) A home or other physical address, including street name and name of a city or town.
> (3) An e-mail address.
> (4) A telephone number.
> (5) A social security number.
> (6) Any other identifier that permits the physical or online contacting of a specific individual.
> (7) Information concerning a user that the Web Site or online service collects online from the user and maintains in personally identifiable form in combi nation with an identifier described in this subdivision.

Id. § 22577(a).

5 A *consumer* is defined as "any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." *Id.* § 22577(d).

6 The term *conspicuously post* with respect to a privacy policy shall include posting the privacy policy through any of the following:

> (1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the website.
> (2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the website, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
> (3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the website, and if the text link does one of the following:
> > (A) Includes the word "privacy."
> > (B) Is written in capital letters equal to or greater in size than the surrounding text.
> > (C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.
> (4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.
> (5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

Id. § 22577(b).

7 *Id.* § 22575(a).

8 *Id.* § 22577(b)(5). Section 22575(a) erroneously identifies the relevant section as 22578(b)(5), which does not exist.

9 Effective January 1, 2005, site owners were required to do so under certain circumstances. *See infra* § III.

10 *Id.* § 22575(b).

11 *Id.* § 22576.

12 *Id.* § 22575(a).

13 As a general rule, businesses should keep track of the dates when different versions of their privacy policies were in effect in order to be able to enforce them effectively or defend themselves in litigation or regulatory disputes.

14 *See id.* § 1798.83(c)(1).

15 The term *established business relationship* is defined to mean

> a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, no more than 18 months have elapsed from the date of the purchase, rental, or lease.

Id. § 1798.83(e)(5).

16 *Customer* is defined as "an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes." *Id.* § 1798.83(e)(1).

17 A *disclosure* "means to disclose, release, transfer, disseminate, or otherwise communicate orally, in writing, or by electronic or any other means to any third party." *Id.* § 1798.83(e)(3).

18 The categories of personal information required to be disclosed pursuant to paragraph (1) of subdivision (a) are all of the following:

- Name and address
- Electronic mail address
- Age or date of birth
- Names of children
- Electronic mail or other addresses of children
- Number of children
- The age or gender of children
- Height
- Weight
- Race
- Religion
- Occupation
- Telephone number
- Education
- Political party affiliation
- Medical condition
- Drugs, therapies, or medical products or equipment used
- The kind of product the customer purchased, leased, or rented
- Real property purchased, leased, or rented
- The kind of service provided
- Social security number
- Bank account number
- Credit card number
- Debit card number
- Bank or investment account, debit card, or credit card balance
- Payment history
- Information pertaining to the customer's creditworthiness, assets, income, or liabilities

Id. § 1798.83(e)(6)(A).

19 If a list, description, or grouping of customer names or addresses is derived using any of the categories listed in the preceding footnote, and is disclosed to a third party for direct marketing purposes *in a manner that permits the third party to identify, determine, or extrapolate any other personal information from which the list was derived*, and that personal information when it was disclosed identified, described, or was associated with an individual, the

categories set forth in this subdivision that correspond to the personal information used to derive the list, description, or grouping shall be considered personal information for purposes of the statute. *See id.* § 1798.83(e)(6)(B).

20 *Third party* or *third parties* mean "Third party" or "third parties" means one or more of the following:

- A business that is a separate legal entity from the business that has an established business relationship with a customer;
- A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to section 1798.83(d);
- A business not affiliated by a common ownership or common corporate control with the business required to comply with section 1798.83(a).

Id. § 1798(e)(8).

21 *Direct marketing purposes* means "the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes." *Id.* § 1798.83(e)(2). The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges or obtains consideration for the personal information. *Id.*

Direct marketing purposes does not include the use of personal information

- by bona fide tax exempt charitable or religious organizations to solicit charitable contributions,
- to raise funds from and communicate with individuals regarding politics and government,
- by a third party when the third party receives personal information solely as a consequence of having obtained for consideration permanent ownership of accounts that might contain personal information, or
- by a third party when the third party receives personal information solely as a consequence of a single transaction where, as a part of the transaction, personal information had to be disclosed in order to effectuate the transaction.

Id.

22 Requests must be in writing or email. A business subject to the law must designate the addresses to which requests should be sent. If a business chooses to do so, it may also allow customers to make requests by toll-free telephone or facsimile numbers. *See id.* § 1798.83(b)(1). Businesses subject to the law must (a) notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or means to obtain those addresses or numbers and instruct those employees that customers who inquire about the company's privacy practices or compliance with this law shall be given this information; or (b) add to its home page a link either to a page titled "Your Privacy Rights" (written in a larger type than the surrounding text, or in contrasting type, font, or color, or set off by other marks or symbols that call attention to the language) or add the words "Your Privacy Rights" to a link to the business's privacy policy (in which case other words may appear on the link so long as "Your Privacy Rights" appears in the same size or style), where on the first page a customer's rights pursuant to this section and the designated addresses or numbers are listed; or (c) make the designated addresses or numbers, or means to obtain them, readily available upon request at every place of business in California where the business or its agents regularly have contact with customers. *See id.* § 1798.83(b)(1).

> *Employees who regularly have contact with customers* means
>
> employees whose contact with customers is not incidental to their primary employment duties, and whose duties do not predominantly involve ensuring the safety or health of the businesses customers. It includes, but is not limited to, employees whose primary employment duties are as cashier, clerk, customer service, sales, or promotion. It does not, by way of example, include employees whose primary employment duties consist of food or beverage preparation or service, maintenance and repair of the business' facilities or equipment, direct involvement in the operation of a motor vehicle, aircraft, watercraft, amusement ride, heavy machinery or similar equipment, security, or participation in a theatrical, literary, musical, artistic, or athletic performance or contest.

Id. § 1798.83(e)(4).

23 *See id.* § 1798.83(c)(1).

24 If a request is directed to the business at other than one of its designated addresses or numbers, it must comply within "a reasonable period in light of the circumstances related to how the request was received," but not longer than 150 days from the date received.

25 A business that is required to comply with this statute is not obligated to provide the information associated with specific individuals and may provide the required information in standardized format. *Id.* § 1798.83(b)(3).

26 *Id.* § 1798.83(c)(2).

27 *Id.* § 1798.83(d).

28 *See Cal. Fin. Code* §§ 4050 *et seq.*

29 Cal Civil Code § 1798.83(h).

30 *See id.* § 1798.38(f).

31 *See id.* § 1798.84

32 *Id.* § 1798.84(d).

33 *See id.* § 1798.84(e).

34 *Id.* § 1798.84(f).

35 *Id.* § 1798.84(a).

36 Cal. Civ. Code §§ 1798.29, 1798.82.

37 *Breach of the security system* means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of any personal information maintained by the agency.

38 *See* 15 U.S.C. § 7001.

39 *See* Cal. Bus. & Prof. Code §§ 17200 *et seq.*

40 The phrase *owns or licenses* "is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." *Id.* § 1798.81.5(a).

41 *Personal information* means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the date elements are not encrypted or redacted:

- (A) Social security number.
- (B) Driver's license number or California identification card number.
- (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- (D) Medical information

42 Cal. Bus. & Prof. Code § 1798.81.5(b).

43 For example, in *Chance v. Avenue A, Inc.,* 165 F. Supp. 2d 1153 (W.D. Wash. 2001), the court granted defendants' motion for summary judgment and denied as moot plaintiffs' motion for class certification in a case arising out of defendants' alleged placement of cookies on user computers, permitting user communications to be monitored allegedly without their knowledge. The court granted summary judgment on plaintiffs' Computer Fraud and Abuse Act claim because the minimum $ 5,000 damage requirement had not been met. The court further granted summary judgment on plaintiffs' claim under the stored communications provisions of the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq*. because, given the technological and commercial relationship between users and the defendant's website, it was implausible to suggest that "access" was not intended or authorized. Summary

judgment likewise was granted on plaintiffs' claim under the Wiretap Act, 18 U.S.C.S. § 2510 *et seq*. based on the finding that it was implicit in the code instructing users' computers to contact the website that consent had been obtained to the interception of communication between users and defendants.

Similarly, in *In re Doubleclick Inc. Privacy Litig.,* 154 F. Supp. 2d 497 (S.D.N.Y. 2001), the court granted defendant's motion to dismiss plaintiffs' federal claims, declined to exercise supplemental jurisdiction over plaintiffs' state law claims, and dismissed with prejudice plaintiffs' amended complaint based on various claims arising out of Doubleclick's proposed plan to allow participating websites to exchange cookie files obtained by users to better target banner advertisements. Plaintiffs, Web users, had alleged that defendant's cookies collected information about them, such as names, email addresses, home and business addresses, telephone numbers, searches performed on the internet, and Web pages or sites, which plaintiffs considered personal in nature and that users would not ordinarily expect advertisers to be able to collect. Among other things, the court ruled that because defendant's affiliated websites were the relevant "users" of internet access under the Electronic Communications Privacy Act (ECPA), and submissions containing personal data made by users to defendant's affiliated websites were intended for those websites, the sites' authorization was sufficient to grant defendant's access under 18 U.S.C. § 2701(c)(2).

The court similarly granted defendant's motion to dismiss most federal claims, and declined to exercise supplemental jurisdiction over state law claims in *In re Intuit Privacy Litig.,* 138 F. Supp. 2d 1272 (C.D. Cal. 2001). In that case, which arose out of the collection of data in cookie files, defendant's motion to dismiss claims under 18 U.S.C. § 2511 and 18 U.S.C. § 1030 was granted without prejudice because plaintiffs had failed to sufficiently allege a tortious or criminal purpose, or that they had suffered damage or loss. The motion was denied, however, with respect to plaintiffs' claim under 18 U.S.C. § 2701 for intentionally accessing electronically stored data. *See also, e.g., In re Pharmatrak Privacy Litig.,* 329 F.3d 9 (1st Cir. 2003) (reversing and remanding for further consideration the entry of summary judgment on plaintiffs' claim under the Electronic Communications Privacy Act (ECPA) that their privacy rights had been violated when the defendants' practice of collecting personal information on websites was not disclosed to users). *But see In re Toys R Us, Inc., Privacy Litig.,* MDL No. M-00-1381, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001) (denying a motion to dismiss in a case based on the defendant's alleged use of cookies to collect user data based on the finding that plaintiffs had stated a claim under the Computer Fraud and Abuse Act and granting leave to amend the complaint to assert a Wiretap Act claim).

44 *See In re RealNetworks, Inc. Privacy Litig.,* Civil No. 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 8, 2000) (denying an intervenor's motion for class certification where the court found that RealNetworks had entered into a contract with putative class members that provided for binding arbitration).

45 *See, e.g., Comb v. PayPal, Inc.,* 218 F. Supp. 2d 1165 (N.D. Cal. 2002) (holding a click-through contract that contained an arbitration provision to be substantively and procedurally unconscionable under California law).

46 *See, e.g., Specht v. Netscape Communications, Inc.,* 306 F.3d 17 (2d Cir. 2002) (holding posted terms accessible via a link to not be binding on users because assent was not obtained).